R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 10 JUIN 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

DB 267/141102
ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

REQUÊTE EN DÉLIVRANCE 1/2

Réservé à L'INPI

Cet imprimé est à remplir lisiblement à l'encre noire

REMISE DES PIÈCES DATE 17 JUIL 2002 LIEU 38 INPI GRENOBLE N° D'ENREGISTREMENT 0209072 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE 17 JUIL. 2002 PAR L'INPI	❶ NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE **Cabinet Michel de Beaumont** **1 rue Champollion** **38000 GRENOBLE**
Vos références pour ce dossier *(facultatif)* B5589	

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

❷ NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de Brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet intiale*	☐ N° Date / /

❸ **TITRE DE L'INVENTION (200 caractères ou espaces maximum)**

PARTAGE D'UN OPÉRATEUR LOGIQUE À REGISTRE DE TRAVAIL

❹ **DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE**	Pays ou organisation Date N° Pays ou organisation Date / / N° Pays ou organisation Date / / N° ☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé "Suite"**
❺ **DEMANDEUR**	☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé "Suite"**
Nom ou dénomination sociale	STMicroelectronics SA
Prénoms	
Forme juridique	Société anonyme
N° SIREN	
Code APE-NAF	
ADRESSE Rue	29, Boulevard Romain Rolland
Code postal et ville	92120 MONTROUGE
Pays	FRANCE
Nationalité	Française
N° de téléphone *(facultatif)*	
N° de télécopie *(facultatif)*	
Adresse électronique *(facultatif)*	

PARTAGE D'UN OPÉRATEUR LOGIQUE À REGISTRE DE TRAVAIL

La présente invention concerne, de façon générale, le traitement de mots binaires par des fonctions de calcul. L'invention concerne plus particulièrement l'exécution, par une machine d'états en logique câblée d'un circuit intégré, d'un calcul représentant une fonction susceptible d'être utilisée par plusieurs applications au sein de ce même circuit.

Un exemple d'application de la présente invention concerne l'implémentation, au sein d'un même circuit, de plusieurs traitements ayant tous recours à une même fonction opératoire. Par exemple, il peut s'agir d'un traitement de signature à clé publique, d'un contrôle d'intégrité des données ou d'un générateur aléatoire pour la cryptographie. Dans tous les cas ci-dessus, on a généralement recours à une fonction discriminante dite "fonction de hashage", par exemple, des fonctions connues sous les dénominations SHA, MD5, etc.

La plupart de ces fonctions discriminantes sont basées sur un traitement itératif d'un message découpé en blocs tenant compte du résultat de l'itération précédente. Elles utilisent donc généralement un unique registre de travail qui est mis à jour à chaque itération de l'opération et constitue, en fin de fonction, un registre de sortie fournissant le résultat souhaité (signa-

L'invention vise également à proposer une solution compatible avec la miniaturisation souhaitée des circuits intégrés.

L'invention vise également à permettre un partage de l'opérateur en logique câblée sans nuire au besoin de traitement en temps réel d'une application prioritaire.

Pour atteindre ces objets et d'autres, la présente invention prévoit un circuit de calcul d'une fonction discriminante à itérations successives et à registre de travail sur des données découpées par blocs, comportant :

un unique opérateur en logique câblée d'exécution de la fonction ;

une pluralité de registres de travail partageant ledit opérateur ; et

un élément de sélection d'un des registres de travail pour être associé à l'opérateur.

Selon un mode de réalisation de la présente invention, chaque registre stocke un état courant de l'opérateur et le rang de l'itération correspondante.

Selon un mode de réalisation de la présente invention, ladite fonction est une fonction de hashage.

Selon un mode de réalisation de la présente invention, un multiplexeur constituant l'élément de sélection est commandé par un décodeur de priorité associé à un processeur intégré contenant ledit circuit de calcul.

Ces objets, caractéristiques et avantages, ainsi que d'autres de la présente invention seront exposés en détail dans la description suivante de modes de réalisation particuliers faite à titre non-limitatif en relation avec les figures jointes parmi lesquelles :

la figure 1 représente, de façon très schématique et sous forme de blocs, un mode de réalisation d'un circuit de calcul d'une fonction de discrimination selon la présente invention ; et

Jusque là, ce qui a été décrit correspond à un opérateur câblé d'une fonction discriminante classique. Par exemple, il pourra s'agir d'une fonction dite de hashage.

Selon l'invention, les états d'entrée (PS) et de sortie (CS) de l'opérateur 2 correspondent aux contenus successifs d'un unique registre de travail par application. Toutefois, on prévoit autant de registres de travail 3 (REG1, ..., REGj, ..., REGn) que d'applications devant partager le circuit 1.

Chaque registre 3 est équivalent à un registre de travail classique associé à un opérateur câblé 2. Toutefois, selon l'invention, des entrées/sorties des registres 3 sont reliées aux entrées multiples d'un multiplexeur 4 dont une unique entrée/sortie est reliée en entrée (signal PS) de l'opérateur 2 et en sortie (signal CS) de cet opérateur 2. Le multiplexeur 4 reçoit un signal de sélection (SEL) provenant, par exemple, d'un contrôleur de priorité (non représenté) associé à l'unité centrale de traitement du processeur intégrant le circuit 1.

Les états initiaux IS_1, ..., IS_j, ..., IS_n sont chargés sous contrôle de l'unité centrale dans chaque registre 3. Les états finaux FS_1, ..., FS_j, ...FS_n de la fonction f après les itérations requises sont lus individuellement dans chaque registre, par les circuits du processeur ayant requis l'application de la fonction de hashage à un mot binaire donné.

De façon classique, le nombre m d'itérations dépend du nombre de blocs de données à traiter. Selon l'invention, le nombre n de registres dépend du nombre d'applications qui requièrent l'opérateur 2.

La figure 2 est un organigramme simplifié de la fonction remplie par l'opérateur 2.

On part (bloc 10, IS) d'un état initial. Cet état est, dans l'exemple de la figure 1, préalablement chargé dans l'un des registres de travail associé à l'application ayant requis la fonction. Dans un exemple particulier appliqué à une fonction dite SHA, cet état initial est prédéterminé.

intermédiaires de calcul, l'invention préserve le caractère sécuritaire requis généralement aux applications de fonctions discriminantes.

Un autre avantage de la présente invention est que sa mise en oeuvre est particulièrement simple dans un processeur intégré. En particulier, la mise en oeuvre de l'invention est compatible avec les circuits matériels et les processus de commande généralement utilisés dans des processeurs intégrés. De plus, l'application traitée par l'opérateur 2 est transparente pour ce dernier, en ce sens que tout fonctionne comme s'il n'était connecté qu'à un registre.

Selon un exemple préféré d'application de la présente invention, l'opérateur 2 est partagé par plusieurs applications parmi lesquelles au moins un contrôle d'intégrité de données en temps réel. Dans ce cas, cette application est considérée comme la plus prioritaire.

Une deuxième application potentielle peut être un calcul de signature ou de code d'authentification ayant un rang de priorité moins élevé.

En troisième rang de priorité, on peut prévoir d'utiliser l'opérateur 2 dans la génération d'un nombre pseudo aléatoire qui possède alors le rang de priorité le plus faible.

Bien entendu, la présente invention est susceptible de diverses variantes et modifications qui apparaîtront à l'homme de l'art. En particulier, la réalisation pratique du circuit de calcul selon l'invention est à la portée de l'homme du métier à partir des indications fonctionnelles données ci-dessus. De plus, les commandes nécessaires au multiplexeur et aux différents registres en utilisant des moyens de commande classiques sont à la portée de l'homme du métier. En outre, bien que cela n'ait pas été détaillé, la sélection du bloc B_i affecté au mot de données de l'application pourra être effectuée de plusieurs façons. Par exemple, l'unité centrale de traitement du circuit intégré gère la lecture des blocs voulus selon les priorités décidées.

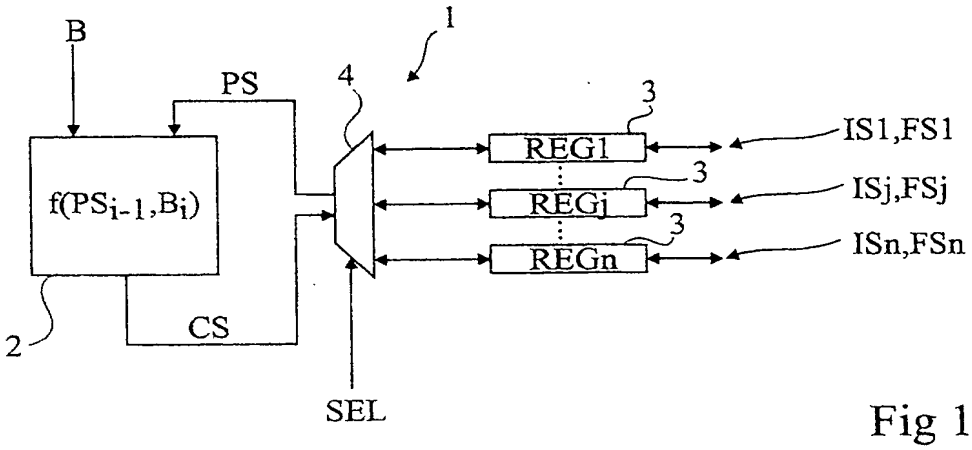
B
PS
1
4
3
REG1
IS1,FS1
3
REGj
ISj,FSj
3
REGn
ISn,FSn
f(PSi-1,Bi)
2
CS
SEL

Fig 1

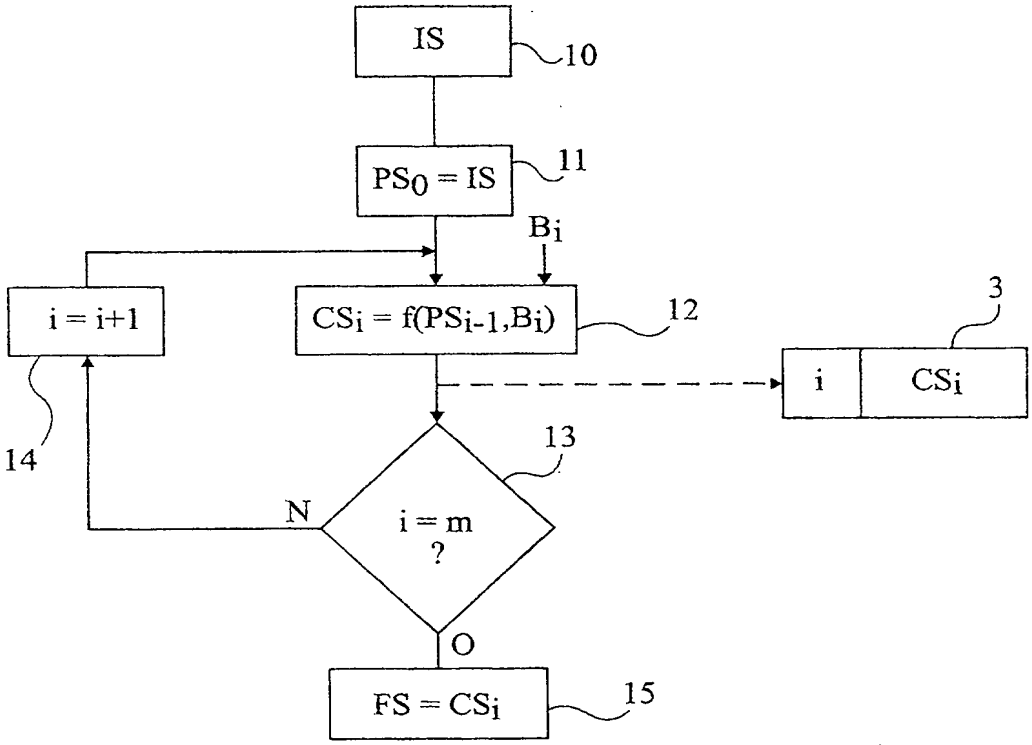
IS
10
PS0 = IS
11
Bi
i = i+1
CSi = f(PSi-1,Bi)
12
3
i
CSi
14
13
N
i = m
?
O
FS = CSi
15

Fig 2